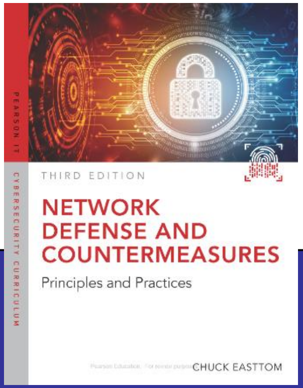
Encryption Fundamentals

Based on slides accompanying the book

Network Defense and Countermeasures

by Chuck Easttom (2018)



Objectives

- Explain encryption concepts
- Describe the history of encryption and modern encryption methods
- Use some simple decryption techniques

Introduction

A basic level of understanding encryption is provided in this chapter.

- ✓ No matter how many firewalls or security instruments are in place, if traffic is not encrypted, it is vulnerable.

Q: Why?

History of Encryption

- Originally used in military communications
- Associated with written communications initially
- Evolved to include telephone, radio, Internet/computer communications
- Encryption methods have become more complicated over the decades

Early Methods of Encryption

- Single-Alphabet Substitution
  - The Caesar Cipher: Shift *key* positions to the right
  - ROT 13: Rotate 13 characters to the right
  - Atbash Cipher: reverse the alphabet

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Q: Issues with Single-Alphabet Substitution?

- Language features are not diffused in the ciphertext.
- Key space is too small.

Early Methods of Encryption

- Multi-Alphabet Substitution

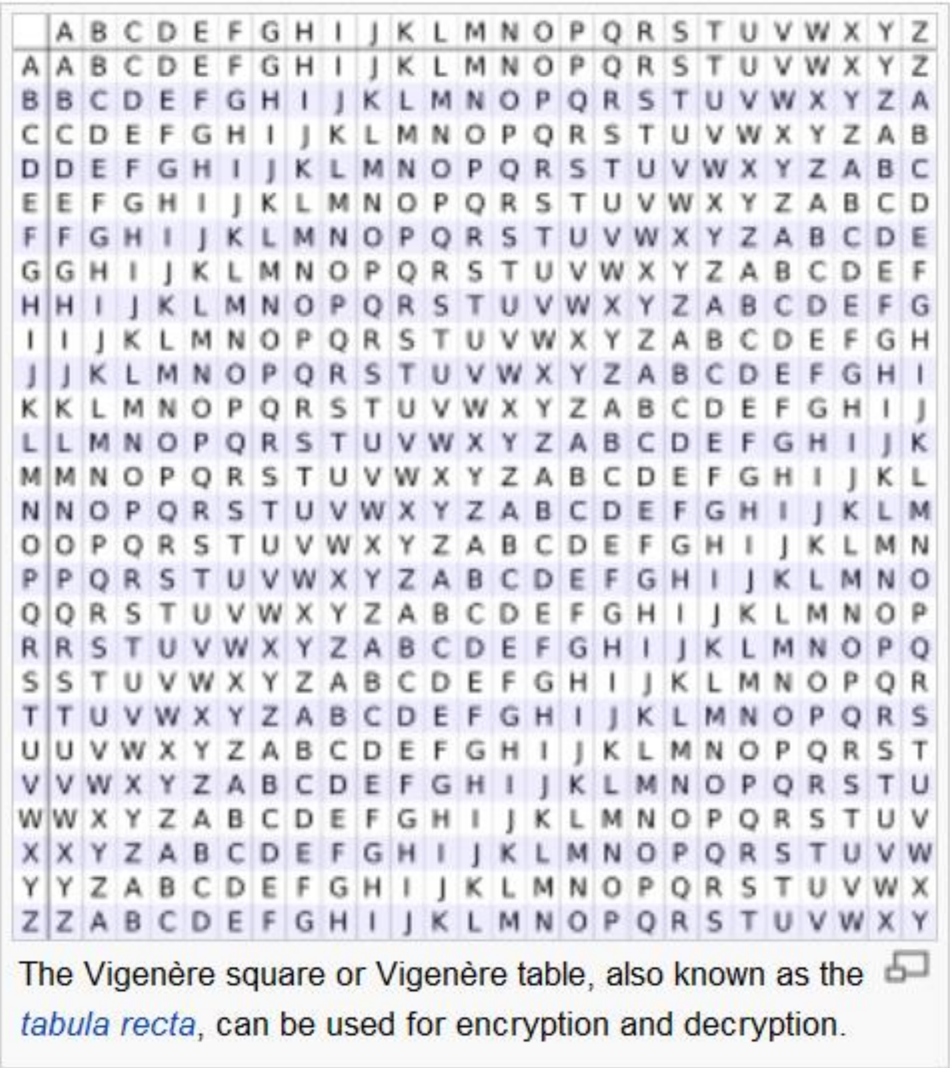
  e.g., Vigenère ciphers

  - Like Cæsar cipher, but use a phrase as the key
  - Example
    - Message `THE BOY HAS THE BALL`
    - Key `VIG`
    - Encipher using Cæsar cipher for each letter:

key	VIGVIGVIGVIGVIGV
plain	THEBOYHASTHEBALL
cipher	OPKWWECIYOPKWIRG

The Vigenère Table

Source: http://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

The Vigenère square or Vigenère table, also known as the *tabula recta*, can be used for encryption and decryption.

- Q: How would the table be used for decryption?

Attacking the Vigenère Cipher

- Approach: the *Kasiski* method

1. Establish period; call it *n*
2. Break message into *n* parts, each part being enciphered using the same key letter
3. Solve each part
   - You can leverage one part from another

Early Methods of Encryption

- Transposition Ciphers

  e.g., Rail Fence Cipher

  - Rearrange letters in plaintext to produce ciphertext
  - Example Rail-Fence Cipher
    - Plaintext is `HELLO WORLD`
    - Rearrange as

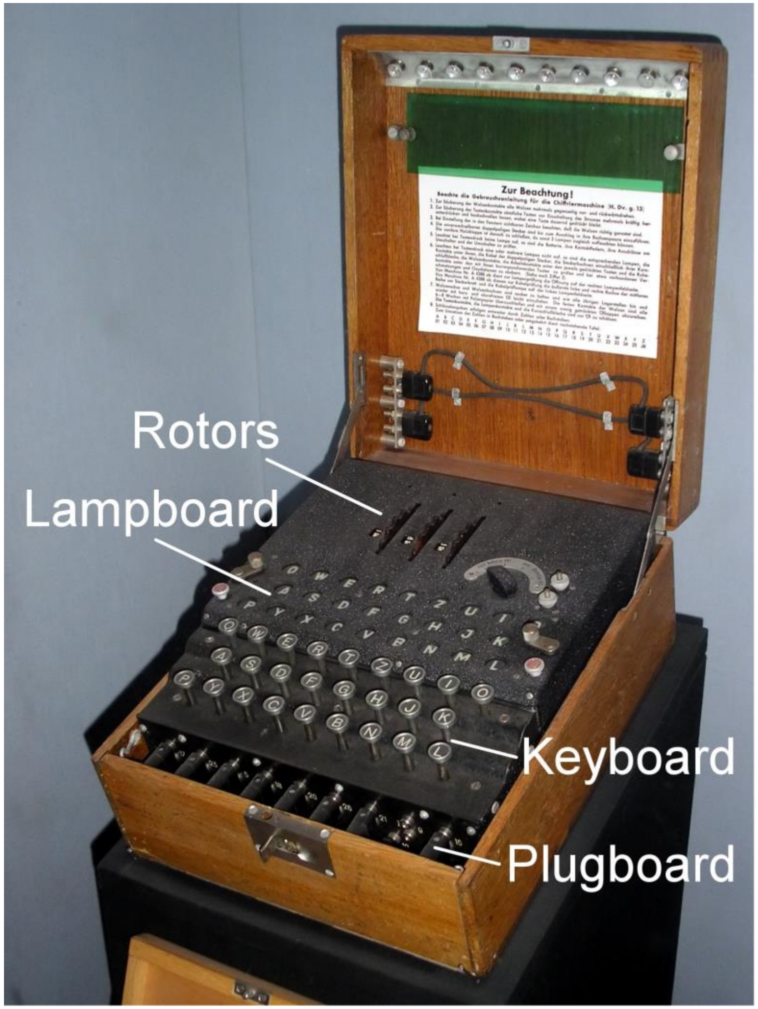
      ```
      HLOOL
      ELWRD
      ```
    - Ciphertext is `HLOOL ELWRD`
    - Question: `What is the key?`

Early Methods of Encryption

- Enigma

Q: Is Enigma a substitution or transposition cipher?

Q: Is it mono-alphabetic or poly-alphabetic?



Early Methods of Encryption

11001010100110010100111010011110010011

- Binary Operations
  - AND – This operation states that 1 AND 1 → 1
  - OR – There must be a 1 (one) in either of the numbers to result in 1 for that position
  - XOR – If a position has 1 in one number but not the other, then the result is 1

- If s1 XOR s2 → s3, then s2 XOR s3 → s1.

Q: How would you prove it?

Additional Information on Cryptography

- http://practicalcryptography.com/ciphers/

- Check out the slides on http://sceweb.uhcl.edu/yang/teaching/csci5233fall2018/

Modern Encryption Methods

- Symmetric Encryption vs Public Key Encryption
  - Symmetric crypto: aka secret-key or shared-key crypto
- Key generation methods
  - Key Stretching
  - PRNG (or Pseudo-Random Number Generator)
- Digital Signatures

Q: Is DS an encryption method?

Symmetric Encryption

- DES
  - Uses a symmetric key system
  - Data is divided and transposed
  - Data is then sent through a series of steps (16 rounds)
  - Further scrambled with a swapping algorithm
  - Finally transposed one last time

- Blowfish
  - Symmetric block cipher
  - Designed in 1993 by Bruce Schneier
  - “Blowfish is a variable-length key, 64-bit block cipher. The algorithm consists of two parts: a key-expansion part and a data-encryption part. Key expansion converts a key of at most 448 bits into several subkey arrays totaling 4168 bytes.” (https://www.schneier.com/academic/archives/1994/09/description_of_a_new.html)

Symmetric Encryption

- Advanced Encryption Standard (AES)
  - Uses Rijndael algorithm
  - Block cipher
  - Specifies three key sizes: 128, 192, and 256 bits
- International Data Encryption Algorithm (IDEA)
- Serpent
- Twofish

Pseudo-Random Number Generators (PRNG)

- Symmetric ciphers need a cipher key; PRNG generates these keys.

- “A **pseudorandom** process is a process that appears to be **random** but is not.”
  - https://en.m.wikipedia.org/wiki/Pseudorandomness

- Example algorithms of ‘**Cryptographically secure pseudorandom number generator**’: https://en.m.wikipedia.org/wiki/Cryptographically_secure_pseudorandom_number_generator

Key Stretching

- “to make a possibly weak **key**, typically a password or passphrase, more secure against a brute-force attack by increasing the resources (time and possibly space) it takes to test each possible **key**” (https://en.wikipedia.org/wiki/Key_stretching)
- Two widely used key stretching algorithms:
  - Password-Based Key Derivation Function 2 (PBKDF2)
    - Part of PKCS #5 v 2.01
    - Applies some function to a password or passphrase along with salt to produce a derived key
  - bcrypt
    - A derivation of the Blowfish algorithm used with passwords

Selecting a Symmetric Encryption Method

- For standard business data, any method should work.
- For large amounts of data, speed is almost as important as security.
- Highly sensitive data should be secure regardless of speed.
- Variable length keys are only important if you need them.
  - For example, when different types of data require different encryption methods/keys.

Public Key Encryption

- One key is used to encrypt (e.g., public key)
- Another is used to decrypt (e.g., private key)
- The two keys are *inverse* of each other.
- You can freely distribute your public key so anyone can encrypt a message to you
- Only you can decrypt the messages
- Slower than symmetric ciphers

Public Key Encryption Methods

- RSA
  - Rivest, Shamir, and Adleman created in 1977
  - Widely used encryption algorithm
- Diffie-Hellman
- ElGamal
- MQV
- Digital Signature Algorithm (DSA)
- Elliptic Curve

Identifying Good Encryption

- Be suspicious of encryption methods that
  - Are advertised as unbreakable
  - Are advertised as certified
  - Are put forth by inexperienced vendors

Digital Signatures

- Digital signatures use asymmetric cryptography in reverse order
- They can verify who sent the message
- Some part of the message is encrypted or signed with the user’s private key
- Any recipient can verify the signature using the sender’s public key
- Note: DS is not an encryption method.

Q: What security service(s) does DS provide?

Digital Certificates

- A digital document that contains a public key (and other information) signed by a trusted third party, a Certificate Authority (CA)
- Distributes a public key securely (against man-in-the-middle attack)
- Provides a means to verify whose public key it is
- X.509
  - An international standard for the format and information contained in a digital certificate

Q: Security services provided by certificates?

Certificate Authorities (CA)

- Primary role is to digitally sign the public key of a given user
- A Registration Authority (RA) is often used to handle verification prior to certificates being issued
- Public Key Infrastructure (PKI)
  - An arrangement that binds public keys with respective user identities by means of a CA
  - A network of trusted CA servers

PGP Certificates

- Pretty Good Privacy (PGP) is a system, not a specific algorithm
- Offers digital signatures, asymmetric encryption, and symmetric encryption
- Often found in e-mail clients
- Uses its own certificate format
- PGP certificates are self-generated, not using a CA

Hashing

- A function that takes a variable-size input and returns a fixed-size string (the *hash value*)
- Hashing is one-way; you cannot un-hash something
- Hashing is how Windows stores passwords
- *Salt* refers to random bits that are used as one of the inputs to the hash
  - Complicates dictionary and rainbow table attacks

NOTE: Hashing is not an encryption method.

Q: What security services are provided by hashing?

Hashing Methods

- Secure Hash Algorithm (SHA)
  - Most widely used
  - SHA-1, SHA-2, SHA-3, SHA-256
- MD5
  - Not collision resistant
- RACE Integrity Primitives Evaluation Message Digest (RIPEMD)
- HAVAL

Cracking Passwords

- Administrators can use password crackers to test their own systems’ defenses
- John the Ripper – well-known cracking app
- Rainbow tables
- Other password crackers
  - Russian password crackers: www.password-crackers.com/crack.html
  - Password recovery: www.elcomsoft.com/prs.html
  - LastBit password recovery: http://lastbit.com/mso/Default.asp

John the Ripper

- Found at www.openwall.com/john/
- A free download
- Works with password files, not live passwords
- Password file is stored in different places depending on the operating system
- Cracked passwords are stored in a file named john.pot

General Cryptanalysis

- *Cryptanalysis*: The science of trying to find alternate ways to break cryptography
- Usually not very successful
- Can be quite tedious, with no guarantee of success

- Methods
  - Brute force
  - Frequency analysis
  - Known plaintext
  - Chosen plaintext
  - Related key attack
  - Birthday attack
  - Differential cryptanalysis
  - Linear cryptanalysis

Steganography

- *Steganography*: The art and science of writing hidden messages in such a way that nobody other than the sender and intended recipient suspects the existence of the message.
- Message is often hidden in some other file such as a digital picture or audio file.
- Messages do not attract attention to themselves.

Steganography

- Key Terms
  - *Payload*: The data to be covertly communicated
  - *Carrier*: The signal, stream, or data file into which the payload is hidden
  - *Channel*: The type of medium used (e.g., photos, video, audio)
- Tools Available
  - QuickStego
  - Invisible Secrets
  - MP3Stego
  - Stealth Files 4
  - SNOW

Steganalysis

- *Steganalysis*: Detecting hidden messages
- Raw Quick Pair (RQP) method
  - for analyzing an image to detect hidden messages
- Chi-square analysis
  - calculates the average Least Significant Bit (LSB), …
- Examining noise distortion in audio carrier files

Quantum Computing and Quantum Cryptography

- Quantum computing allows more values than binary states
- Quantum based algorithms are superior at factoring large numbers
  - Widely used RSA algorithm is based on the difficulty of factoring a large number into its prime factors
  - When factoring becomes less difficult, RSA will be obsolete
- Other algorithms may also become obsolete

“NIST is publishing **NIST Internal Report (NISTIR) 8240, *Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process*.**”

- https://csrc.nist.gov/News/2019/pqc-standardization-process-2nd-round-candidates

Summary

- Encryption had simple beginnings
- Those beginnings fostered more complex mathematical structures that can be used for encryption
- Modern encryption methods are very complex algorithms

Summary

- Modern encryption methods can be symmetric or asymmetric
  - Symmetric uses a single key for encryption and decryption
  - Asymmetric uses a public key and a private key
- Symmetric methods include DES, Blowfish, AES, IDEA, Serpent, and Twofish

Summary

- Asymmetric methods (Public Key Encryption) include RSA, Diffie-Hellman, ElGamal, MQV, DSA, and Elliptical Curve
- No encryption is unbreakable or certified
- Digital signatures use asymmetric cryptology in reverse order
- Digital certificate validate user identity
- Certificate authorities provide trusted verification of certificates

Summary

- PGP digital certificates do not use certificate authorities
- Hashing takes a variable-size input and returns a fixed-size string
  - MD5 and SHA are common hashes
  - Other hashes include RIPEMD and HAVAL
- Decryption (without the proper key) is difficult and not usually successful

Summary

- Passwords can be cracked with utilities such as John the Ripper or with Rainbow tables
- Cryptanalysis attempts to break cryptography
    - Methods include brute force, frequency analysis, known plaintext, chosen plaintext, related key attack, birthday attack, differential cryptanalysis, and linear cryptanalysis
- Steganography is the art/science of placing hidden messages within seemingly ordinary files, such as graphics or audio clips

Summary

- Quantum computing introduces additional states besides binary on/off states.
- Quantum-based algorithms may make it easier to crack encoding and may render current cryptography methods obsolete

→ NIST is trying to standardize next-generation crypto methods against these threats.